State of Alabama

Information Technology (IT) Dictionary

Revision A

Introduction

This document defines all of the terms, abbreviations, and acronyms used in the State of Alabama information technology (IT) documentation (policies, procedures, plans, guidelines, etc.) including the Resource Access Control Facility (RACF) Security Administrator's Guide. The document(s) where each defined term is utilized is identified following its definition.

Acronyms and Abbreviations

- A -	
AAA	Authentication, Authorization, and Accounting
ABC	Alcoholic Beverage Control [Board]
ABI	Alabama Bureau of Investigation
ACEE	Accessor Environment Element
ACJIC	Alabama Criminal Justice Information Center
ACK	Acknowledge (receipt of a packet in TCP)
ACL	Access Control List
ADPH	Alabama Department of Public Health
AES	Advanced Encryption Standard
AO	Authorizing Official
AOC	Administrative Office of Courts
AP	Access Point
AS	Authentication Server
ASP	Application Service Provider
ATAC	Agency Technology Advisory Committee
AV	Anti-Virus
- B -	
BEM	Bid Evaluation Matrix
- C -	
CA	Certification Authority
CCB	Configuration Control Board
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CHAP	Challenge Handshake Authentication Protocol
CI	Configuration Item
CICS	Customer Information Control System
CIDR	Classless Inter-Domain Routing
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CPE	Customer Premise Equipment
CPU	Central Processing Unit
CSIRT	Cyber Security Incident Response Team

- D -	
DAC	Discretionary Access Control
DASD	Direct Access Storage Device
DBA	Database Administrator
DBMS	Database Management System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHR	Department of Human Relations
DIR	Department of Industrial Relations
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Name System (or Service)
DNSSEC	Domain Name System Security Extensions
DOS	Denial of Service
DOT	Department of Transportation
DPS	Department of Public Safety
DSMON	Data Security Monitor
DSS	Data Security Standard

- E -	
EPROM	Erasable Programmable Read-Only Memory

- F -	
FAR	False Acceptance Rate
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FPGA	Field Programmable Gate Array
FR	Frame Relay
FRR	False Rejection Rate
FSP	File Security Packet
FTP	File Transfer Protocol
FWSM	Firewall Services Module
FY	Fiscal Year

- G -	
GDG	Generation Data Group
GID	Group Identifier

- H -	
HFS	Hierarchical File System
HIPAA	Health Information Portability and Accounting Act
HSSI	High-Speed Serial Interface
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transmission Protocol, Secure

- I -	
IA	Information Assurance
IAS	Internet Accessible Segment
ICAC	Internet Crimes Against Children
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	IP Security
IPT	IP Telephony
ISA	Internet Security and Acceleration
ISD	Information Systems Division
ISDN	Integrated Services Digital Network
ISN	Initial Sequence Number
ISO	Information Security Officer
ISP	Internet Service Provider
IT	Information Technology
ITB	Invitation to Bid
IV&V	Independent Verification and Validation

- J -

- K -

- L -	
LAN	Local Area Network
LU	Logical Unit

- M -	
MAC	Mandatory Access Control
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MPLS	Multi-Protocol Label Switching
MS-ISAC	Multi-State Information Sharing and Analysis Center
MVS	Multiple Virtual Storage

- N -	
NA	Network Administrator
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NSA	National Security Agency

- O -	
OIDCARD	Operator Identification Card

OS	Operating System
OSS	Open Source Software

- P -

PBX	Private Branch Exchange
PCI	Payment Card Industry
PDA	Personal Digital Assistant
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point of Sale
PSC	Public Service Commission

- Q -

- R -

RACF	Resource Access Control Facility
RAID	Redundant Array of Independent Disks
RAS	Remote Access Server
RCP	Remote Copy; command on the Unix OS
RDP	Remote Desktop Protocol
RFP	Request for Proposal
RRMP	Residual Risk Mitigation Plan
RSA	An encryption algorithm named after its creators: Rivest, Shamir, and Adleman;
RSH	Remote Shell
RSN	Robust Security Network

- S -

SA	System Administrator
SAN	Storage Area Network
SCP	Secure Copy; command on the Unix OS
SCSI	Small Computer System Interface
SDLC	Systems Development Life Cycle
SE	Secure Erase®
SER	Security Evaluation Request
SFTP	Secure FTP
SIP	Session Initiated Protocol
SME	Subject Matter Expert
SMF	System Management Facility
SP	Software Programmer
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSLF	Specialized Security – Limited Functionality

STIG	Security Technical Implementation Guide
SYN	Synchronize (packet in TCP)
- T -	
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSIG	Transaction Signature
TSO	Time Sharing Option
- U -	
UACC	Universal Access Authority
UID	User Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
- V -	
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding
VTC	Video Tele-Conferencing
- W -	
WAN	Wide Area Network
WD	Web Developer
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
- X -	
XML	Extensible Markup Language
- Y -	
- Z -	

Definitions

- A -

ACCESS: The ability to use a protected resource. [*z/OS Security Server RACF Security Administrator's Guide*]

ACCESS AUTHORITY: See ACCESS LEVEL

ACCESS CONTROL: Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner. [*State IT Guideline 660-02G5*]

ACCESS LEVEL: The capability (NONE, EXECUTE, READ, UPDATE, CONTROL or ALTER) a User ID has for a specific protected resource (DATASET or other resource). [*z/OS Security Server RACF Security Administrator's Guide*]

ACCESSOR ENVIRONMENT ELEMENT (ACEE): A control block that contains a description of the User ID's current security environment. An ACEE is created during user identification and authentication. [*z/OS Security Server RACF Security Administrator's Guide*]

ACCOUNTABILITY: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. [*State IT Guideline 660-02G5*]

ADVANCED ENCRYPTION STANDARD (AES): AES is a symmetric block cipher algorithm using cryptographic key sizes of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. WPA2 is an implementation of AES. [*State IT Standard 680-03S1*]

ADWARE: A software application that can display advertising banners while the program is running or via some other triggering mechanism is called adware. Ad delivery systems are most often integrated into free applications as a way for developers to recover costs or generate revenue. A critical eye has been placed on adware system since in many cases, in addition to downloading ads, they may also upload user information collected without explicit permission. This type of adware is often referred to as "trackware" or "spyware". [*State of Alabama Cyber Security Plan 2009*]

APPROVED EMAIL: Includes all email systems supported by Information Services Division (ISD), Department of Finance. [*State IT Standard 680-01S1*]

ASSURANCE: Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass. [*State IT Guideline 660-02G5*]

ASYMMETRIC CRYPTOSYSTEM: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (public-key encryption). [*State IT Standard 680-03S1*]

AUDITOR ATTRIBUTE: A user attribute that allows the user to specify logging options and list any profile (including its auditing options). [*z/OS Security Server RACF Security Administrator's Guide*]

AUTHENTICATION: Verifying the identity of a subject requesting the use of a system and/or access to a resource. [*State IT Standard 620-03S1; State IT Guideline 660-02G5; z/OS Security Server RACF Security Administrator's Guide*]

AUTHORITY: The right to access objects, resources or functions. [*z/OS Security Server RACF Security Administrator's Guide*]

AUTHORIZATION: The granting or denying of access rights to a user, program, or process. [*State IT Guideline 660-02G5*]

AUTHORIZATION CHECKING: The action of determining whether a User ID is permitted access to a protected resource. [*z/OS Security Server RACF Security Administrator's Guide*]

AVAILABILITY: The property of being accessible and usable upon demand by an authorized entity. [*State IT Standard 680-01S1; State IT Guideline 660-02G5*]

AWARENESS LEVEL TRAINING: Creates the sensitivity to the threats and vulnerabilities and the recognition of the need to protect data, information, and the means of processing them. [*State IT Standard 610-01S1*]

- B -

BASELINE: Specific rules or settings necessary to implement required security controls consistently throughout the enterprise (e.g., the specific system settings required to harden a server or secure a workstation operating system). [*State IT Procedure 600-03P2*]

BIOMETRIC TEMPLATE: The digital representation of information captured during enrollment. [*State IT Standard 620-03S2*]

BOTNET: A network of malware-infected machines, a collection of software robots or bots, which run autonomously and can be remotely controlled as a group usually for nefarious purposes. [*State of Alabama Cyber Security Plan 2009*]

BYPASS: When someone circumvents one or more components of the biometric system, most probably the capture device because it is outside the perimeter of the protected system or area. An attacker might compromise the capture hardware or wiring to send electronic or digital representations of biometric data directly to the comparator without first presenting a sample to the capture device. [*State IT Standard 620-03S2*]

- C -

CAPTURE: Biometric technology is used to record a user's physical characteristic or behavior. The hardware performing the reading is called the *capture device*. Capture devices typically are designed to capture one biometric characteristic such as a finger print, retina pattern or keyboard dynamic. [*State IT Standard 620-03S2*]

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. [*State IT Standard 640-02S1*]

CICS: See CUSTOMER INFORMATION CONTROL SYSTEM

CICS SEGMENT: The portion of a RACF profile containing data for the Customer Information Control System (CICS) product. [*z/OS Security Server RACF Security Administrator's Guide*]

CLASSLESS INTER-DOMAIN ROUTING (CIDR): An IP addressing scheme that replaces the scheme based on classes A, B, and C. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations. CIDR was created to help reduce problems associated with IP address depletion. [*State IT Guideline 660-02G2*]

CLEAR: Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. [*State IT Standard 680-01S4*]

COLLATERAL INFORMATION: Information that is in the workspace that is not meeting or conference related but can be seen by the camera or heard by the microphone. Collateral information can also be non meeting/conference related information on a PC workstation that is used to participate in, or present to, a conference. [*State IT Guideline 660-02G7*]

COMPARISON: The live sample and biometric template are provided as inputs to a software module known as the comparator, which generates a score describing how close a match the two are to one another. Based on predetermined thresholds, the two are either declared a match given the resulting score (*acceptance*) or they are not (*rejection*). The determination is forwarded to whatever access control system the biometric technology is supporting. [*State IT Standard 620-03S2*]

CONFIDENTIALITY: A concept that applies to data that must be held in confidence and describes the status or degree of protection that must be provided for such data. [*State IT Standard 680-01S1; State IT Guideline 660-02G5*]

CONFIGURATION ITEM (CI): A product that is placed under configuration management. Such products may include hardware components, software components, documentation, or any other item that needs to be controlled. [*State IT Guideline 600-05G1*]

CONFIGURATION MANAGEMENT (CM): From an information security point of view, configuration management is a process that provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications, [*State IT Guideline 600-05G1*]

COOKIES: Small text files which a web server may ask the web browser to store and send back to the web server when needed. Cookies may be used to store a transaction identifier or other information a user may provide. [*State IT Standard 1210-00S1: Online Privacy and Data Collection*]

CUSTOMER INFORMATION CONTROL SYSTEM (CICS): A program licensed by IBM that provides online transaction processing services and management for critical business applications. [*z/OS Security Server RACF Security Administrator's Guide*]

CYBER SECURITY INCIDENT: An assessed occurrence having actual impact (i.e., damage is done, access is achieved by an intruder, loss occurs, or malicious code is implanted), or potentially adverse effects on an information system (e.g., when detecting something noteworthy or unusual such as a new traffic pattern, new type of malicious code, a source of persistent attacks, or evidence of inappropriate use having the potential to impact the organization). [*State IT Procedure 600-04P1*]

- D -

DASD: See DIRECT ACCESS STORAGE DEVICE

DATA INTEGRITY: The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. [*State IT Guideline 660-02G5*]

DATA SECURITY: The protection of data and resources from unauthorized disclosure, modification or destruction, whether accidental or intentional. [*z/OS Security Server RACF Security Administrator's Guide*]

DATA SECURITY MONITOR (DSMON): A RACF auditing tool that produces reports verifying an installation basic system integrity and data security controls. [*z/OS Security Server RACF Security Administrator's Guide*]

DATASET PROFILE: A profile that provides RACF protection for one or more data sets. [*z/OS Security Server RACF Security Administrator's Guide*]

DELEGATION: The act of giving other users or groups the authority to perform RACF operations. [*z/OS Security Server RACF Security Administrator's Guide*]

DENIAL OF SERVICE (DOS): The prevention of authorized access to resources or the delaying of time-critical operations (time-critical may be milliseconds or it may be hours, depending upon the service provided). [*State IT Guideline 660-02G5*]

DENIAL OF SERVICE ATTACK: Multiple service requests sent to a victim's computer until it eventually overwhelms the system causing it to freeze, reboot, and ultimately not be able to carry out regular tasks. [*State IT Procedure 600-04P1*]

DES: Cryptographic algorithm designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46. DES only supports key lengths of 56 bits which is considered inadequate. [*State IT Standard 680-03S1*]

DIGITAL CERTIFICATE: A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. [*z/OS Security Server RACF Security Administrator's Guide*]

DIGITAL FORENSICS: The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. [*State IT Procedure 600-04P2*]

DIRECT ACCESS STORAGE DEVICE (DASD): A general term for magnetic disk storage devices. The term has historically been used in the mainframe and minicomputer (mid-range computer) environments and is sometimes used to refer to hard disk drives for personal computers. A redundant array of independent disks (RAID) is also a type of DASD. The "direct access" means that all data can be accessed directly in about the same amount of time rather than having to progress sequentially through the data. A type of storage device, such as a magnetic disk, in which bits of data are stored at precise locations, enabling the computer to retrieve information directly without having to scan a series of records. [*z/OS Security Server RACF Security Administrator's Guide*]

DISCRETIONARY ACCESS CONTROL (DAC): a means of restricting access to objects based on the identity of the accessor, or groups to which the accessor belongs. The controls are discretionary in that an accessor who has a high-enough access authority can allow another accessor to access the object. [*z/OS Security Server RACF Security Administrator's Guide*]

DOMAIN: See SECURITY DOMAIN.

DOMAIN NAME: A domain name is all the text that follows the first period '.' in a host name. A host name is used to locate an entity on the Internet. A host name is part of a Uniform Resource Locator

(URL), which is the address of a site or document on the Internet. [*State IT Standard 1200-00S1: Domain Naming and Registration*]

DUAL HOMING: Network topology in which a device is connected to the network by way of two independent access points (e.g., wired and wireless). [*State IT Standard 640-02S1*]

- E -

EMAIL: See APPROVED EMAIL

ENROLLMENT: The initial association of an identity with a biometric characteristic. [*State IT Standard 620-03S2*]

ENTERPRISE CLIENT: Environment consisting of an Active Directory® domain with member servers and domain controllers that run Windows Server 2003/2008 and client computers running Windows 2000 and newer OS. [*State IT Baseline 660-02B1*]

ENTITY: Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). [*State IT Guideline 660-02G5*]

ERASE ON SCRATCH: The physical overwriting of data on a DASD data set when the data is deleted (scratched). [*z/OS Security Server RACF Security Administrator's Guide*]

- F -

FILE PERMISSION BITS: In OpenEdition MVS (see MULTIPLE VIRTUAL STORAGE), information about a file that is used, along with other information, to determine if a process has read, write or execute/search permission to a file. The bits are divided into three parts: owner, group and other. Each part is used with the corresponding file class of processes. [*z/OS Security Server RACF Security Administrator's Guide*]

FILE SECURITY PACKET (FSP): In OpenEdition MVS, a control block containing the security data (file's owner uid, owner gid and the permission bits) associated with the file. [*z/OS Security Server RACF Security Administrator's Guide*]

FILE SECURITY PACKET (FSP): In z/OS UNIX, a control block containing the security data associated with the file. [*z/OS Security Server RACF Security Administrator's Guide*]

FILE TRANSFER PROTOCOL (FTP): In the Internet suite of TCP/IP related protocols, an application layer protocol that transfers bulk data files between machines or hosts. [*z/OS Security Server RACF Security Administrator's Guide*]

- G -

GAMBLING: Sites where a user can place a bet or participate in a betting pool, participate in a lottery, or receive information, assistance, recommendations, or training in such activities. Does not include sites that sell gambling-related products/machines or sites for offline casinos and hotels, unless they meet one of the above requirements. [*State IT Standard 630-05S1*]

GENERAL RESOURCE PROFILE: A profile that provides RACF protection for one or more general resources. [*z/OS Security Server RACF Security Administrator's Guide*]

GENERATION DATA GROUP (GDG): a collection of data sets with same base name that are kept in chronological order. [*z/OS Security Server RACF Security Administrator's Guide*]

GROUP IDENTIFIER (GID): A number between 0 and 2147483647 that identifies a group of users to the z/OS UNIX. [*z/OS Security Server RACF Security Administrator's Guide*]

GROUP PROFILE: A set of RACF-defined User IDs that share a common purpose or function. [*z/OS Security Server RACF Security Administrator's Guide*]

GUIDELINE: Typically a collection of system specific or procedural specific "suggestions" for best practice, not required, but strongly recommended. [*State IT Procedure 600-03P2*]

- H -

HASH ALGORITHM (or HASH FUNCTION): A function that maps a bit string of arbitrary length to a fixed length bit string. [*State IT Standard 680-03S1*]

HIERARCHICAL FILE SYSTEM (HFS): Where information is organized in a tree-like structure of directories. Each directory can contain files or other directories. [*z/OS Security Server RACF Security Administrator's Guide*]

HIGH-IMPACT: The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

> Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.
>
> A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:
>
> > (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
> >
> > (ii) result in major damage to organizational assets;
> >
> > (iii) result in major financial loss; or
> >
> > (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

[*State IT Standard 600-04S1; Source of Origin: FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems*]

HYPERTEXT LINK: Element on a Web page (text, image, or file) that when clicked opens another Web page or jumps to another location. [*State IT Standard 1210-00S4: Hypertext Linking*]

- I -

IDENTIFYING INFORMATION: Any information used either alone or in conjunction with other information that specifically identifies a person or a person's property, and includes, but is not limited to, any of the following information related to a person:

- Name

- Date of birth
- Social Security number
- Driver's license number
- Financial services account numbers, including checking and savings accounts
- Credit or debit card numbers
- Personal identification numbers (PIN)
- Electronic identification codes
- Automated or electronic signatures
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage
- Any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services

[*The Code of Alabama, Section 13A-8-191 (Act 2001-312, p. 399, §2)*]

IDENTITY: Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain. [*State IT Guideline 660-02G5*]

IEEE 802.11i: The security specification of the 802.11 standard consisting of two components: IEEE 802.1x and Robust Security Network (RSN). RSN is used to establish a secure wireless connection between wireless devices. RSN uses dynamic negotiation of authentication and encryption algorithms between access points and wireless devices. The authentication schemes are based on IEEE 802.1x and EAP with Advanced Encryption Standard (AES) as the encryption algorithm. [*State IT Standard 640-03S1*]

IMPLEMENTATION LEVEL TRAINING: Provides the ability to recognize and assess the threats and vulnerabilities to automated information resources so that the responsible managers can set security requirements which implement agency security policies. [*State IT Standard 610-01S1*]

INDIVIDUAL: A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. State of Alabama employees are “individuals.” Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities, are not “individuals.” [*State IT Standard 680-013S2*]

INDIVIDUAL ACCESS CONTROLS: Methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. [*State IT Standard 680-01S1*]

INDIVIDUAL IDENTIFIER: Information associated with a single individual and used to distinguish him or her from other individuals (e.g., name, Social Security number or other identifying number, symbol, or other identifying particular such as a finger or voice print or photograph). [*State IT Standard 680-013S2*]

INFORMATION OWNERS: Individual, or group of individuals, responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be. Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the asset. [*State IT Policy 680-01*]

INTEGRATED SERVICES DIGITAL NETWORK (ISDN): A circuit-switched telephone network system that allows digital transmission of voice and data over ordinary telephone copper wires. [*State IT Standard 640-02S1*]

INTEGRITY: The property that data or information has not been modified or altered in an unauthorized manner. [*State IT Standard 680-01S1; State IT Guideline 660-02G5*]

IPSEC: Internet Protocol Security (IPsec) is a framework for a set of protocols for security at the network or packet processing layer of network communication designed to provide private communications over public networks. [*State IT Standard 640-02S2*]

IT SECURITY ARCHITECTURE: A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments. [*State IT Guideline 660-02G5*]

- J -

- K -

KERNEL: The part of z/OS UNIX that provides support for such services as UNIX I/O, process management and general UNIX functionality. [*z/OS Security Server RACF Security Administrator's Guide*]

KEY: In cryptography, a sequence of symbols that is used with a cryptographic algorithm for encrypting or decrypting data. See private key and public key. [*z/OS Security Server RACF Security Administrator's Guide*]

KEY RING: A named collection of certificates for a specific user or server application used to determine the trustworthiness of a client. [*z/OS Security Server RACF Security Administrator's Guide*]

- L -

LEGACY CLIENT: Environment consisting of an Active Directory® directory service domain with member servers and domain controllers that run Windows Server 2003/2008 and some client computers that run Microsoft Windows 98 and Windows NT® 4.0. Computers running Windows 98 must have the Active Directory Client Extension (DSClient) installed. [*State IT Baseline 660-02B1*]

LIVE SAMPLE: The digital representation of information captured during verification. [*State IT Standard 620-03S2*]

LOG: A record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. [*State IT Standard 670-06S1*]

LOGGING: The recording of audit data about specific events. [*z/OS Security Server RACF Security Administrator's Guide*]

LOGICAL UNIT (LU): A port providing formatting, state synchronization and other high-level services through which an end user communicates with another end user over an SNA network. [*z/OS Security Server RACF Security Administrator's Guide*]

- M -

MALWARE: Short for malicious software (such as a virus or Trojan horse); software designed specifically to damage or disrupt a system. [*State IT Standard 630-03S1*]

MANDATORY ACCESS CONTROL (MAC): A means of restricting access to objects on the basis of the sensitivity of the information contained in the objects and the formal authorization (clearance) of subjects to access information of such sensitivity. [*z/OS Security Server RACF Security Administrator's Guide*]

MASK: A technique to provide protection against casual viewing of a password that has been defined or altered, when an encryption function is not available. [*z/OS Security Server RACF Security Administrator's Guide*]

MEDIA: Refers to different types of data storage options including but not limited to paper, microforms, hand-held devices (cell phones, personal digital assistants, palm devices), networking devices, floppies, hard drives, USB removable devices with or without hard drives (including pen drives, thumb drives, flash drives, memory sticks), ZIP disks, magnetic tapes, optical disks, and memory. [*State IT Standard 680-01S4*]

MOBILE CODE: Software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. [*State IT Standard 660-01S1*]

MODERATE-IMPACT: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of moderate and no security objective is assigned a potential impact value of high.

> The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
>
> Serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:
>
> > (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
> >
> > (ii) result in significant damage to organizational assets;
> >
> > (iii) result in significant financial loss; or
> >
> > (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

[*State IT Standard 600-04S1; Source of Origin: FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems*]

MULTIPLE VIRTUAL STORAGE (MVS): The mainframe operating system that allows multiple users to work simultaneously using the full amount of virtual storage. [*z/OS Security Server RACF Security Administrator's Guide*]

- N -

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST): A non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. [*http://www.nist.gov/index.html*]

NETWORK SCANNING: The gathering of data on information system and device configurations, which may be used for system identification, maintenance, security assessment and investigation, vulnerability compliance, or compromise. This includes network port scanning and vulnerability scanning, whether wired or wireless. [*State IT Standard 670-01S3*]

NON-DISCLOSURE AGREEMENT (NDA): A legal contract between at least two parties outlining sensitive or confidential materials the parties wish to share with one another for certain purposes, but wish to restrict from generalized use. In other words, it is a contract through which the parties agree not to disclose information covered by the agreement. [*State IT Standard 680-01S1*]

NON-REPUDIATION: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. [*State IT Standard 680-01S1*]

- O -

OBJECT: A passive entity that contains or receives information. Note that access to an object potentially implies access to the information it contains. [*State IT Guideline 660-02G5*]

OMVS SEGMENT: The portion of a RACF profile containing OMVS logon information. [*z/OS Security Server RACF Security Administrator's Guide*]

ONLINE GAMES: Sites that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. Includes magazines dedicated to video games and sites that support or host online sweepstakes and giveaways. [*State IT Standard 630-05S1*]

OPERATIONS ATTRIBUTE: A user attribute that grants the equivalent of ALTER access to all data sets unless the user or one of the user's connect groups appears explicitly in the access list of a data set's profile. If a user needs to perform maintenance activities on DASD volumes, granting DASDVOL authority to those volumes using the PERMIT command is preferred over assigning the OPERATIONS or group-OPERATIONS attribute. Note that most modern DASD maintenance programs do not require the OPERATIONS attribute. [*z/OS Security Server RACF Security Administrator's Guide*]

OPERATOR IDENTIFICATION CARD (OIDCARD). A small card with a magnetic stripe encoded with unique characters and used to verify the identity of a terminal operator to RACF. [*z/OS Security Server RACF Security Administrator's Guide*]

OWNER: The user or group that creates a profile, or is specified as the owner of a profile. The owner can modify, list, or delete the profile. [*z/OS Security Server RACF Security Administrator's Guide*]

- P -

PASSPHRASE: A sequence of words or other text used to control access to a computer system, program or data; similar to a password in usage, but generally longer for added security and easier to remember because it's based on words or a phrase that means something to the user. [*State IT Standard 620-03S1*]

PASSWORD: A string of characters known to a user who must specify it to gain full or limited access to a system and to the data stored within it. RACF uses a password to verify the identity of the user. [*z/OS Security Server RACF Security Administrator's Guide*]

PERFORMANCE LEVEL TRAINING: Provides the employees with the skill to design, execute, or evaluate agency computer security procedures and practices. The objective of this training is that employees will be able to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications. [*State IT Standard 610-01S1*]

PERMISSION BITS: In z/OS UNIX, part of security controls for directories and files stored in the z/OS UNIX file system. Used to grant read, write, search (just directories), or execute (just files) access to owner, file or directory owning group, or all others. [*z/OS Security Server RACF Security Administrator's Guide*]

PERSONAL DIGITAL ASSISTANT (PDA): Personal electronic email and Smartphone devices such as Blackberry, Treo, and other handheld communication devices that have similar inherent features and vulnerabilities. [*State IT Standard 660-02S2*]

PERSONALLY IDENTIFIABLE INFORMATION (PII): Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. [*State IT Standard 680-013S2*]

PICONET: An ad-hoc computer network of devices using Bluetooth technology protocols to allow one master device to interconnect with up to seven active slave devices. [*State IT Standard 640-03S3*]

PII ELECTRONIC RECORD: Any item, collection, or grouping of information in electronic form that associates personal information such as education, financial transactions, medical history, criminal or employment history, with an individual identifier. Also any item, collection, or grouping of information in electronic form that associates two or more individual identifiers (e.g., name and social security number). Electronic records that contain information about education, financial transactions, medical history, or criminal or employment history but do not include individual identifiers are not considered PII electronic records. [*State IT Standard 680-013S2*]

POLICY: The overall expression of management's intention on how security should be implemented, maintained, and enforced. Policies are usually point-specific, covering a single area, and outline specific responsibilities that must be met. [*State IT Procedure 600-03P2*]

POLICY LEVEL TRAINING: Provides the ability to understand computer security principles so that executives can make informed policy decisions about their computer and information security programs. [*State IT Standard 610-01S1*]

PRINCIPLE: A rule or standard, especially of good behavior. [*State IT Guideline 660-02G5; American Heritage Dictionary*]

PRIVATE KEY: In public key cryptography, a key that is known only to its owner. Contrast with public key. [*z/OS Security Server RACF Security Administrator's Guide*]

PROCEDURE: A set of instructions or methods for performing a specific task or function. One or more procedures may support the implementation of a security policy. [*State IT Procedure 600-03P2*]

PROFILE: A RACF record containing information for a User ID, group dataset or General Resource. Information in the RACF profile is used by RACF to protect resources and determine appropriate access and capabilities. See DATASET PROFILE, GENERAL RESOURCE PROFILE, GROUP PROFILE, and USER PROFILE. [*z/OS Security Server RACF Security Administrator's Guide*]

PROTECTED ATTRIBUTE: User ID without a password or OIDCARD. User ID is used for submitting jobs to the mainframe via submitting software (i.e. CA7). [*z/OS Security Server RACF Security Administrator's Guide*]

PROTECTED RESOURCE: A resource defined to RACF for the purpose of controlling access to the resource. Some of the resources that can be protected by RACF are DASD volumes, tape volumes, load modules, terminals, IMS and CICS transactions, and installation-defined resource classes. [*z/OS Security Server RACF Security Administrator's Guide*]

PROTECTED USER ID: A user ID that cannot enter the system by any means that requires a password or passphrase, and cannot be revoked by incorrect password and passphrase attempts. Assigning a protected user ID to z/OS UNIX, a UNIX daemon, or another important started task or subsystem assures that the ID cannot be used for other purposes, and that functions will not fail because the ID has been revoked. [*z/OS Security Server RACF Security Administrator's Guide*]

PUBLIC KEY: In public key cryptography, a key that is made available to everyone. Contrast with private key. [*z/OS Security Server RACF Security Administrator's Guide*]

PUBLIC KEY CRYPTOGRAPHY: Cryptography in which public keys and private keys are used for encryption and decryption. One party uses a common public key and the other party uses a secret private key. The keys are complementary in that if one is used to encrypt data, the other can be used to decrypt it. [*z/OS Security Server RACF Security Administrator's Guide*]

PURGE: Purging is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was on the media before purging. The goal is to destroy the data beyond forensic recovery. [*State IT Standard 680-01S4*]

PUSH EMAIL: A delivery system with real-time capability to "push" email through to the client device as soon as it arrives, rather than requiring the client to poll and collect or pull mail manually. [*State IT Standard 660-02S2*]

- Q -

- R -

RACF: See RESOURCE ACCESS CONTROL FACILITY

RACF DATABASE: The repository for the security information that RACF maintains. [*z/OS Security Server RACF Security Administrator's Guide*]

RACF DATASET: One of the data sets comprising the RACF database. [*z/OS Security Server RACF Security Administrator's Guide*]

RACF-INDICATED: Pertaining to a data set for which the RACF indicator is set on. If a data set is RACF-indicated, a user can access the data set only if a RACF profile or an entry in the global access-checking table exists for that data set. On a system without RACF, a user cannot access a RACF-indicated data set until the indicator is turned off. For VSAM data sets, the indicator is in the catalog entry. For non-VSAM data sets, the indicator is in the data set control block (DSCB). For data sets on tape, the indicator is in the RACF tape volume profile of the volume that contains the data set. [*z/OS Security Server RACF Security Administrator's Guide*]

RACF REPORT WRITER: A RACF function that produces reports on system use and resource use from information found in the RACF SMF records. However, the preferred method for producing RACF SMF reports is the RACF SMF data unload utility (IRRADU00). [*z/OS Security Server RACF Security Administrator's Guide*]

RACF SMF DATA UNLOAD UTILITY (IRRADU00): A RACF utility that enables installations to create a sequential file from the security-relevant audit data. The sequential file can be viewed directly, used as input for installation-written programs, and manipulated with sort/merge utilities. It can also be uploaded to a database manager (such as DB2) to process complex inquiries and create installation-tailored reports. See SMF RECORDS. [*z/OS Security Server RACF Security Administrator's Guide*]

RADIUS: Remote Authentication Dial-In User Service, RADIUS, is an authentication, authorization, and accounting (AAA) protocol for network access application. [*State IT Standard 640-02S2*]

REDUNDANT ARRAY OF INDEPENDENT DISKS (RAID): A method of storing data on multiple hard disks. When disks are arranged in a RAID configuration, the computer sees them all as one large disk. Placing data on multiple disks improves input/output performance and increases fault tolerance. [*State IT Guideline 660-01G3*]

REPLAY ATTACK: When someone is able to capture a valid user's biometric data and then use it at a later time for authorized access. The attacker may obtain the biometric data from the stored biometric template or as it is being transmitted from one element of the biometric system to another (e.g., the capture device to the comparator). [*State IT Standard 620-03S2*]

REMEDIATION DATABASE: A database of vulnerability patches, instructions, workarounds, etc. that need to be applied within the organization. Enterprise patch management tools usually supply such a database, but there may be a need to manually maintain a separate one for IT technologies not supported by the patch management tool. [*State IT Standard 670-03S1*]

RESOURCE ACCESS CONTROL FACILITY (RACF): A program (licensed by IBM) that provides access control by identifying and verifying the users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, logging unauthorized attempts to enter the system, and logging detected accesses to protected resources. RACF is included in the Security Server and is available as a separate program for the MVS and VM environments. [*z/OS Security Server RACF Security Administrator's Guide*]

RESOURCE: Any system parameter such as dataset, DASD volumes, tape volumes, terminals, and system software products such as IMS, CICS, ROSCOE and TSO. See DATASET PROFILE and GENERAL RESOURCE PROFILE. [*z/OS Security Server RACF Security Administrator's Guide*]

RESOURCE PROFILE: A profile that provides RACF protection for one or more resources. USER, GROUP, and CONNECT profiles are not resource profiles. The information in a resource profile can include the profile name, profile owner, universal access authority, access list, and other data. Resource

profiles can be discrete profiles or generic profiles. [*z/OS Security Server RACF Security Administrator's Guide*]

RESTRICTED ATTRIBUTE: A user attribute that can be assigned to prevent the user ID from being used to access protected resources it is not specifically authorized to access. Restricted users cannot gain access to protected resources through global access checking, UACC, or an ID(*) entry on the access list, and optionally, to a z/OS UNIX file system object through the 'other' bits. RESTRICTED User ID that must specifically defined to a resource in order to utilize the resource. [*z/OS Security Server RACF Security Administrator's Guide*]

REVOKE ATTRIBUTE: A user attribute that prevents a RACF-defined user from entering the system. [*z/OS Security Server RACF Security Administrator's Guide*]

REVOKED: User ID that no longer has the ability to sign onto the mainframe. [*z/OS Security Server RACF Security Administrator's Guide*]

RISK: The net mission/business impact considering (1) the likelihood that a particular threat source will exploit or trigger a particular information system vulnerability and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to:

- Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information.
- Non-malicious errors and omissions.
- IT disruptions due to natural or man-made disasters.
- Failure to exercise due care/diligence in the implementation and operation of the IT.

[*State IT Guideline 660-02G5*]

RISK ANALYSIS: The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. [*State IT Guideline 660-02G5*]

RISK MANAGEMENT: The ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level or risk. [*State IT Guideline 660-02G5*]

RSA: An asymmetric key encryption algorithm based on factoring very large integers. Asymmetric algorithm keys must be longer for equivalent resistance to attack than symmetric algorithm keys. 1024-bit RSA keys are equivalent in strength to 80-bit symmetric keys, 2048-bit RSA keys to 112-bit symmetric keys and 3072-bit RSA keys to 128-bit symmetric keys. RSA are the initials of the three algorithm creators: Rivest, Shamir, and Adleman. [*State IT Standard 680-03S1*]

- S -

SCATTER-NET: A set of piconets connected through sharing devices. [*State IT Standard 640-03S3*]

SECURE ERASE (SE): A data-destroy command amounting to "electronic data shredding." SE is built into the hard disk drive itself and is implemented in all ATA interface drives with capacities greater than 15 GB manufactured after 2001. Executing the SE command causes a drive to internally completely erase all possible user data record areas by overwriting with binary zeroes. "HDDerase", a freeware utility that

executes the SE command, is available from: http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml. [*State IT Standard 680-01S4*]

SECURE SHELL (SSH): A computer program and an associated network protocol designed for logging into and executing commands on a networked computer; providing secure encrypted communications between two untrusted hosts over a non-secure network. SSH is most commonly used in combination with SFTP, as a secure alternative to FTP or in combination with SCP, as a secure alternative to RCP file transfers in Unix environments. [*State IT Standard 680-03S1*]

SECURITY: Security is a system property. Security is much more than a set of functions and mechanisms. IT security is a system characteristic as well as a set of mechanisms that span the system both logically and physically. [*State IT Guideline 660-02G5*]

SECURITY CONTROLS: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Security controls are defined in NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems. [*State IT Standard 670-02S1*]

SECURITY DOMAIN: A set of subjects, their information objects, and a common security policy. [*State IT Guideline 660-02G5*]

SECURITY GOALS: Confidentiality, availability, integrity, accountability, and assurance. [*State IT Guideline 660-02G5*]

SECURITY PLAN: A document identifying the system, the sensitivity of information handled by the system, and system security measures including operational, technical, and management controls, system rules of behavior, risk assessment, and any security awareness and training requirements. [*State IT Procedure 600-03P1*]

SECURITY POLICY: The statement of required protection of the information objects. [*State IT Guideline 660-02G5*]

SECURITY SERVICE: A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication. [*State IT Guideline 660-02G5*]

SMF: See SYSTEM MANAGEMENT FACILITY

SMF RECORDS: (1) Records and system or job-related information collected by the System Management Facility (SMF) and used in billing users, reporting reliability, analyzing the configuration, scheduling jobs, summarizing direct access volume activity, evaluating data set activity, profiling system resource use, and maintaining system security. (2) Variable-length process or status records from the SMF data set that are written to the SMF log data set. These records vary in layout based on the type of system information they contain. See RACF SMF DATA UNLOAD UTILITY. [*z/OS Security Server RACF Security Administrator's Guide*]

SOCIAL ENGINEERING: The art of getting people to do things they would not ordinarily do for someone they do not know (such as giving someone their password). Common social engineering methods include posing as a new employee seeking help or as a vendor or employee of a partner company. Common targets of social engineers are receptionists and administrative assistants because they are predisposed to being helpful. [*State IT Procedure 600-04P1*]

SOFTPHONE: Systems which implement VoIP using an ordinary PC with a headset and special software. [*State IT Standard 640-04S1*]

SPECIAL ATTRIBUTE: A user attribute that gives the user full control over all of the RACF profiles in the RACF database and allows the user to issue all RACF commands, except for commands and operands related to auditing. [*z/OS Security Server RACF Security Administrator's Guide*]

SPECIALIZED SECURITY – LIMITED FUNCTIONALITY (SSLF): The SSLF environment consists of an Active Directory domain with member servers and domain controllers that run Windows Server 2003/2008 and clients that run Windows 2000 and newer OS. The SSLF security settings in Microsoft's "Windows Server 2003 Security Guide" track closely with the security level historically represented in the guidelines offered by NSA, NIST, and the security community. However, the SSLF settings are so restrictive that many applications may not function. This may affect server performance and make it more of a challenge to manage the servers. Also, client computers that are not secured by the SSLF policies could experience communication problems with client computers and servers that are secured by the SSLF policies. [*State IT Baseline 660-02B1*]

SPLIT TUNNELING: Term used to describe a multiple-branch networking path. In a VPN context, a secure tunnel is established to the VPN concentrator and other traffic is sent directly to different remote locations without passing through the VPN concentrator. This can expose the State's networked resources to attack and can make State resources accessible to anyone from non-trusted networks. [*State IT Standard 640-02S2*]

SPYWARE: Secret code hidden in an otherwise harmless program. Spyware permits unauthorized access to a computer, allowing someone else to observe the user, read data, or even control the computer. [*State of Alabama Cyber Security Plan 2009*]

SPYWARE EFFECTS: Sites to which spyware reports its findings or from which it alone downloads advertisements. Also includes sites that contain serious privacy issues, such as "phone home" sites to which software can connect and send user info; sites that make extensive use of tracking cookies without a posted privacy statement; and sites to which browser hijackers redirect users. [*State IT Standard 630-05S*]

SPYWARE/MALWARE SOURCES: Sites which distribute spyware and other malware. This includes drive-by downloads; browser hijackers; dialers; intrusive advertising; any program which modifies your homepage, bookmarks, or security settings; and keyloggers. It also includes any software which bundles spyware as part of its offering. [*State IT Standard 630-05S*]

SQL INJECTION: A type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data. [*State IT Guideline 660-01G1*]

SSL VPN: Secure Sockets Layer (SSL) Virtual Private Network (VPN) is a form of VPN that can be used with a standard Web browser. In contrast to the IPsec VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. [*State IT Standard 640-02S2*]

STANDARD: A collection of system-specific or subject-specific requirements that must be met by everyone subject to the source policy. For example, a policy may address the high-level responsibilities for network/system authentication, whereas one or more standards would address the specific requirements for different methods of authentication (passwords, biometrics, etc.). [*State IT Procedure 600-03P2*]

SUBJECT: An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. [*State IT Guideline 660-02G5*]

SUPERUSER: In z/OS UNIX, a system user who operates with the special privileges needed to perform a specified administrative task. [*z/OS Security Server RACF Security Administrator's Guide*]

SUPERUSER AUTHORITY: In z/OS UNIX, the unrestricted authority to access and modify any part of the operating system, usually associated with the user who manages the system. [*z/OS Security Server RACF Security Administrator's Guide*]

SYMMETRIC CRYPTOSYSTEM: A method of encryption in which the same key is used for both encryption and decryption of the data (secret key encryption). [*State IT Standard 680-03S1*]

SYSTEM INTEGRITY: The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. [*State IT Guideline 660-02G5*]

SYSTEM INTERCONNECTION: The direct connection of two or more IT systems for the purpose of sharing data and other information resources. [*State IT Standard 640-01S1*]

SYSTEM LIFE-CYCLE: A circular process model based on the concept that a mission need is defined and translated into an advantageous solution, which goes through a continuous loop of evolution and improvement until it is retired. There are five basic phases of the system life cycle (described in NIST Special Publication 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems):

- Initiation,
- Development/acquisition,
- Implementation,
- Operation/maintenance, and
- Disposition

[*State IT Guideline 660-02G5*]

SYSTEM MANAGEMENT FACILITY (SMF): The part of the operating system that collects and records system and job-related information used in billing users, reporting reliability, analyzing the configuration, scheduling jobs, summarizing direct access volume activity, evaluating data set activity, profiling system resource use, and maintaining system security. The information is recorded in the SMF log data set. [*z/OS Security Server RACF Security Administrator's Guide*]

- T -

THREAT: Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events. [*State IT Guideline 660-02G5*]

THREAT ANALYSIS: The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment. [*State IT Guideline 660-02G5*]

THREAT SOURCE: Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability. [*State IT Guideline 660-02G5*]

TRIPLE DES: Block cipher formed from the DES cipher by using it three times. Triple DES is also known as TDES or 3DES, however, there are variations of TDES which use two different keys (2TDES) and three different keys (3TDES) therefore the non-standard abbreviation 3DES is considered confusing

and should be avoided. In general TDES with three different keys (3TDES) has a key length of 168 bits: three 56-bit DES keys (with parity bits 3TDES has the total storage length of 192 bits), but due to the meet-in-the-middle attack the effective security it provides is only 112 bits. 2TDES is weaker and not recommended because two of the three keys used are identical. [*State IT Standard 680-03S1*]

- U -

UNIVERSAL ACCESS AUTHORITY (UACC): The default access authority that applies to a resource if the user or group is not specifically permitted access to the resource, unless the user is restricted. The universal access authority can be any of the access authorities. [*z/OS Security Server RACF Security Administrator's Guide*]

USER: A person who requires the services of a computing system. [*z/OS Security Server RACF Security Administrator's Guide*]

USER IDENTIFIER (UID): A number between 0 and 2147483647 that identifies a user to z/OS UNIX. The UID is associated with a RACF user ID when it is specified in the OMVS segment of the user profile. A UID is used to identify a system user IN z/OS UNIX. When the identity of the user is associated with a process, a UID value is referred to as a real UID, an effective UID, or an (optional) saved set UID. [*z/OS Security Server RACF Security Administrator's Guide*]

USER ATTRIBUTE: The extraordinary privileges, restrictions, and processing environments assigned to a user. The user attributes are SPECIAL, AUDITOR, CLAUTH, OPERATIONS, GRPACC, ADSP, and REVOKE. [*z/OS Security Server RACF Security Administrator's Guide*]

USER CERTIFICATE: A type of certificate managed by RACF. See DIGITAL CERTIFICATE. [*z/OS Security Server RACF Security Administrator's Guide*]

USER DATASET: A data set defined to RACF in which either the high-level qualifier of the data set name or the qualifier supplied by an installation exit routine is a RACF user ID. [*z/OS Security Server RACF Security Administrator's Guide*]

USER IDENTIFICATION (USER ID): A unique set of numbers, letters and or special characters that identifies a person, process or function. A string of 1–8 alphanumeric characters that uniquely identifies a RACF user, procedure, or batch job to the system. For TSO users, the user ID cannot exceed 7 characters and must begin with an alphabetic, #, $, or @ character. The user ID is defined by a user profile in the RACF database and is used as the name of the profile. [*z/OS Security Server RACF Security Administrator's Guide*]

USER IDENTIFICATION AND AUTHENTICATION: The act of identifying and verifying a user to the system during logon or batch job processing. [*z/OS Security Server RACF Security Administrator's Guide*]

USER IDENTIFICATION AND VERIFICATION: See USER IDENTIFICATION AND AUTHENTICATION

USER PROFILE: A description of a RACF-defined user that includes the user ID, user name, default group name, password, passphrase, profile owner, user attributes, and other information. A user profile can include information for subsystems such as TSO and DFP. [*z/OS Security Server RACF Security Administrator's Guide*]

- V -

VIRTUAL KEY RING: The set of certificates for a specific user or server application used to determine the trustworthiness of a client or peer entity. In contrast to the key ring, the virtual key ring is not added to RACF as a key ring and contains no private keys. The most common type is the CERTAUTH virtual key ring, which is used when an application uses a key ring to validate the certificates of others but has no need for its own certificate and private key. [*z/OS Security Server RACF Security Administrator's Guide*]

VOICE OVER INTERNET PROTOCOL (VoIP): Also referred to as IP Telephony, Internet telephony, Broadband telephony, Broadband Phone, and Voice over Broadband, is the routing of voice conversations over the Internet or through any other IP-based network. [*State IT Standard 640-04S1*]

VIRTUAL PRIVATE NETWORK (VPN): Protected information system link utilizing tunneling, security controls, and end-point address translation giving the impression of a dedicated line. [*State IT Standard 680-03S1*]

VULNERABILITY: A weakness in system security requirements, design, implementation, or operation, that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy. [*State IT Guideline 660-02G5*]

- W -

WPA2: Wi-Fi Protected Access (WPA) is used to secure wireless (Wi-Fi) computer networks. WPA2 implements the full IEEE 802.11i standard and replaces Wired Equivalent Privacy (WEP). [*State IT Standard 680-03S1*]

- X -

- Y -

- Z -

z/OS: A program licensed by IBM that not only includes and integrates functions previously provided by many IBM software products, including the MVS operating system, but also: (1) is an open, secure operating system for IBM enterprise servers, (2) complies with industry standards, (3) is based on the new 64-bit z/Architecture®, and (4) supports technology advances in networking server capability, parallel processing, and object-oriented programming. [*z/OS Security Server RACF Security Administrator's Guide*]

z/OS UNIX SYSTEM SERVICES (z/OS UNIX): The set of functions provided by the shells, utilities, kernel, file system, debugger, Language Environment, and other elements of the z/OS operating system that allows users to write and run application programs that conform to UNIX standards. [*z/OS Security Server RACF Security Administrator's Guide*]

Document History

Version	Release Date	Comments
Original	6/23/2009	
Rev A	7/7/2009	Deleted first definition of PROFILE; modified RACF definition of PROFILE. Changed GROUP to GROUP PROFILE and modified.